DRAFT

The Honorable Dave McCurdy
Committee on Science and Technology
House of Representatives
Washington, D.C. 20515

Dear Congressman McCurdy:

I understand that the Committee on Science and Technology will consider in the near future a bill, H.R. 2889, that provides for a computer security research program and training of federal employees involved in the management, operation and use of computers. The Administration has taken a position in opposition to the bill on the grounds that the government already has in place a mechanism to educate employees on computer security and to conduct research into computer vulnerability. The Agency supports this position. Nevertheless, should the House decide to move forward with this bill, we would urge you to consider a few minor changes so as to preserve the authority of the Director of Central Intelligence to continue the Agency's own very strict computer security program in accordance with established guidelines.

As reported out of the House Government Affairs Committee, the provisions of the bill granting the National Bureau of Standards (NBS) sole authority and responsibility for establishing and conducting computer security management, research and training programs would apply to computers that are subject to the provisions of §111 of the Federal Property and Administrative Services Act of 1949 or Chapter 35 of title 44, United States Code. Since the Agency is exempt from the Federal Property and Administration Act and the provisions of Chapter 35 of title 44 that pertain to computer and telecommunication systems, we would not be affected by enactment of Section 3 or 4 of the bill. However, section 5 of the bill, which mandates that every federal agency provide mandatory training in computer and telecommunication security, would apply to the Agency. The type of training to be given to federal employees would be set out in regulations issued by the Office of Personnel Management (OPM).

We our concerned that section 5 of the bill could be interpreted to require that all agencies follow a single set of regulations regarding the training of employees in computer security. The Agency currently has a very rigorous program to educate our employees on computer security awareness and good security practice. This mandatory computer security program is more stringent than other agencies that do not regularly deal in classified information. A single set of regulations to cover all federal agencies that does not accommodate the particular security needs of individual agencies is not the most effective means to provide the necessary protection needed for computers containing our nation's most sensitive secrets. To ensure that the Agency may continue its own computer security program even though it may be more stringent than the regulations set forth by OPM, we would urge you to recommend that the committee report on this provision make clear that the regulations set forth by OPM on computer security are minimum standards and that federal agencies may decide to exceed those standards for computers that store highly classified data.

The Agency is also concerned with Section 6 of the bill, as reported out of the House Government Operations Committee. Section 6 of the bill mandates that each federal agency take an inventory of computers that store sensitive but unclassified information and develop a plan for the security of the computers and related telecommunication systems. The plan would then be submitted to NSA and NBS for comment, and be subject to disapproval by the General Services Administration (GSA). Because the Agency does have computers that store unclassified but sensitive information, enactment of this provision would require that the Agency submit its plans for protecting these computers to NSA, NBS and GSA. One problem with having to submit security plans for advice, comment and approval is that such plans and programs are frequently in flux. Each time a change is made in the security plan, we would have to report the plan to NSA and NBS, and await the approval of GSA. To delay instituting a new security procedure while awaiting for what is sure to be a slow advice, comment and approval process would unnecessarily jeopardize security. More importantly, we have serious reservations about disclosing security systems which may themselves be classified even though the material they protect is unclassified but sensitive. The bill contains no provisions for protecting or limiting the distribution of these plans and procedures. Without such limitations on the distribution of our security plans, the possibility of compromise of such plans is increased.

Our concerns with respect to Section 6 of the bill were alleviated during the mark-up of the bill by the Subcommittee on Transportation, Aviation and Materials of the House Science and Technology Committee. The subcommittee amended the provision so as to make it applicable to computers subject to §111 of the Federal Property and Administrative Services Act or Chapter 35 of title 44, United States Code. Since the Agency is exempt from these provisions, Section 6 of the bill as reported out of the subcommittee on Transportation, Aviation, and Materials would not affect the Agency. If, despite the Administration's objections, the House moves forward on this legislation we would strongly urge you to support the language in Section 6 of the bill as amended by the subcommittee on Transportation, Aviation and Materials, rather than the language contained in Section 6 of the bill as reported out of the House Government Operations Committee.

If you or your staff have any questions regarding the position of the CIA on this legislation, please do not hesitate to contact me or [redacted] of my staff at [redacted] STAT

The Office of Management and Budget has advised that there is no objection to the submission of this report from the standpoint of the Administration's program.

Sincerely,

[redacted] STAT

Director, Office of Legislative Liaison